(19) FEDERAL REPUBLIC OF GERMANY

GERMAN PATENT OFFICE

(12) **Patent Application Publication**

(10) **DE 197 18 103 A 1**

(51) Int. Cl.[6]:
H 04 L 9/32
H 04 Q 7/38

(21) File code: 197 18 103.1
(22) Filing date: 4/29/1997
(43) Date of publication: 6/4/1998

Application published with the consent of the applicant pursuant to § 31 Para. 2 Number 1 PatG

(71) Applicant:
Schmitz, Kim, 80809 Munich, DE

(72) Inventor:
same as applicant

(74) Representative:
Frhr. von Gravenreuth and Partner, 80336 Munich

The following information is taken from the documents provided by the applicant

(54) Procedure for authorization in a data transmission system

(57) The invention concerns a process and a system for authorization in data transmission systems using a transaction number (TAN) or a comparable password, whereby in a first step the user transmits to an authorization computer through a data input device his identification and/or an identification code for the data input device together with the request for generation or select of a TAN or comparable password from a file, in a second step the authorization computer generates or selects from a file the TAN or comparable password, in a third step the authorization computer transmits the TAN or the comparable password through a different transmission path than in step 1 to a receiver (e.g. mobile phone or pager), in a fourth step the user accepts this TAN or comparable password from the receiver and inputs it into the data input device, in a fifth step this TAN or comparable password is again transmitted to the authorization computer, in a sixth step the authorization computer checks the validity of the TAN or comparable password, in order then in a seventh step to establish or permit a connection between the data input device and a receiving unit.

Description

The invention concerns a process for authorization data transmission systems.

It is known that in telebanking the user needs both his permanent password (PIN) and also a transaction number (TAN) for each individual transaction. Such TANs are transmitted to the user in large blocks. Thus there is a risk that third parties may obtain knowledge of such TANs and, in combination with the password, perform abuse. The risk is increased by the fact that the validity of such TANs is not limited in time.

Call-back systems are also known in which the system called uses a call back, generally to a stored number, to ensure that the calling system is authorized and that a foreign system is not posing as an authorized system. The disadvantage of call-back systems is that an unauthorized user who has gained functional access from any source to the authorized calling system can work under this illegally obtained authorization with no problems, since the call-back system only checks whether it has been called from a basically authorized system.

The invention solves the task of providing a procedure for authorization in data transmission in which security is increased. This process is solved by the invention by the characterizing part of Claim 1.

Wireless telecommunications devices, such as mobile telephones or pagers, often have the capability of receiving short numeric or alphanumeric messages (e.g. the Short Message Service or SMS service) and displaying them on their displays. The present invention uses this capability in order to transmit a TAN or comparable password.

According to the present invention, the user transmits over a data input device his identification (user ID, password, or similar) and/or an identification code for the data input device, together with a request for generation of a TAN (or a comparable password) to a computer which handles the authorization process, and which will hereinafter be called the authorization computer for short. In this authorization computer, a random generator is used to generate an alphanumeric or simple numeric TAN (or comparable password) or one is taken from a file. Then the authorization computer, in parallel with the existing connection with the data input device, over a different transmission path, sends this TAN (or comparable passowrd) to a receiver. This receiver may be, for example,

a) a radio receiver with a display or monitor, like a mobile phone, a pager (e.g. a Cityruf receiver)
b) a specially designed receiver card within the data input device which is addressed via radio or a wired connection,
c) a mailbox,
d) a fax machine, or
e) a speech output device like a fixed speaker or (speech) telephone.

The authorization computer has the necessary telephone, radio phone, or fax numbers, email addresses, or network address(es) for this purpose. The data for this purpose aregenerally stored in the authorization computer. However, it would be possible for the authorization computer to retrieve this information from a database located on a different computer. The authorization computer may even use the invented process to access this other computer.

The authorized user can manually enter the TAN (or comparable password) transmitted in this manner into his data input device and send it back to the authorization computer. In the automated procedure, the invention specifies an automatic transmission of the TAN (or comparable password). The authorization computer now checks the match between all valid TANs (or compable passwords) which it has assigned, and after this authorization check can enable a release of the data flow between the data input device and a receiving unit.

The TAN (or comparable password) may be a TAN for one-time use only. However, other limitations on the validity of the TAN (or comparable password) are also possible, such as the time of user and/or the number or size of the files transferred.

After establishment of an authorized connection in the manner mentioned above, data can now be transmitted from the data input device to the receiving unit (or vice versa; full duplex).

It is obvious that this data can be encrypted for additional security.

Both the data input device and the authorization computer and receiving unit can be normal (personal) computers. The invention works independent of platform, that is, it is independent of processor type, operating system, and/or control electronics (e.g. in the receiving unit) and/or input/out units (e.g. in the data input device and receiving unit).

The security of the system lies in the fact that only after authorization of the unit can data transmission from the data input device to the receiving unit be permitted by the authorization computer. This is achieved by means of the use of separate transmission paths between the data input device and the authorization computer on the one hand, and the authorization computer and the TAN transmission on the other hand. Thus the invention differs from call-back systems in which a check is only made between the data input device and the authorization computer.

The invented process enables a variety of security levels.

At the lowest security level provided by the invention, a radio receiver is built into the data input device as the reciever, for instance in the form of a pluggable card, so that only with this concrete device is data transmission possible to the receiving unit. To increase this security, it can be provided that this radio receiver can only be operated with a user identification element, such as a magnetic or chip card. The user identification element can also work with graphical methods, such as the checking of a fingerprint or image identification of the user.

The additional security level provided by the invention is provided when the authorization computer transmits the TAN (or comparable password) to a pager or comparable device. In that case, authorization takes place only when the data input device and the pager

are in the possession of the same person. Only then is it possible for the TAN (or comparable password) shown on the display of the pager to be entered into the data input device and transmitted from there to the authorization computer.

Data transmitted to a pager can, however, be overheard, as is known. An additional security level provided by the invention can be achieved in that matching encryption modules are in use in the authorization computer and the pager.

Instead of the pager or mobile phone, the invention also provides for the use of a different receiving unit. This can be a mailbox, a fax machine, or a speech output unit. As speech output units according to the invention, fixed speakers or the transmission of speech to a defined telephone connection are possible. For speech output units, there is a spoken output of the TAN (or comparable password).

It is obvious that the transmission to this type of receiving unit can be encrypted.

If instead of a pager a mobile phone, particularly a GSM mobile phone, is in use, then due to the encryption of this transmission technology the invention provides that additional encryption mechanisms can be omitted. In that case, the display of the TAN (or comparable password) takes place on the display of the mobile phone.

Another security level provided by the invention can be achieved by establishing a connection between the data input device and the authorization computer only if an appropriate password is transmitted through the data input device. According to the invention, this password may have a longer time of validity than the TAN.

Another security level provided by the invention can be achieved by requiring a password even for use of the data input device.

It is obvious that a combination of the aforementioned security levels is also possible.

The invention is universally applicable in the area of data transmission systems. This particularly applies, for instance, to the Internet and Intranets, Local Area Networks (LAN), Wide Area Networks (WAN), etc.

The system in question can also be used for physical access control outside of classical data processing. The user can, for instance, enter his personal password on a keypad (=data input device) located in the vicinity of a door. The authorization computer checks this password, where applicable even in connection with access privileges to the actual room – and at the actual time. If the password is (still) valid, the authorization computer transmits the TAN (or comparable password) to a mobile phone or a device functionally equivalent to a pager and specially designed for the door lock system. Then this TAN (or comparable password) is manually entered by the user on the keypad installed in the vicinity of the door, and automatically forwarded to the authorization computer. After a successful check, the authorization computer sends a signal to release the door lock mechanism. This release can, if necessary, be limited in time. The receiving unit can in that case be of very simple design from a technical standpoint, since it only needs to process the signal for the release of the door lock mechanism in such a way that the appropriate electromechanics are released for opening of the door.

Thus it is possible to construct a system in which different people can have different permissions for the entry into different rooms.

The concrete fields of application include, for instance:

- Computer centers
- Airports
- Government agencies
- Customs
- Border crossings
- Safety areas
- Banks
- Treasuries
- Garages
- Parking garages
- Cars

The entire system obtains its security from the combination of multiple different basic principles and factors:

(1) "what you have" (the possibly GSM) chip card, which cannot be duplicated), that is, a physical unit which cannot be give away without loss.
(2) "what you know" (the PIN of the GSM chip card along with the user name in the data input device and/or authentication server), that is, knowledge which cannot be unintentionally or accidentally given away.
(3) DES encryption and cryptographic authentication in the GSM network itself, resulting in resistance to eavesdropping and manipulation attacks.

Thus in order to compromise the system, the combination of at least three – each already very improbable in itself – events are required:

a) physical loss of the (mobile phone) chip card, the pager, or an external access to the mailbox, fax machine, or speech unit,
b) divulgence of the PIN of the receiver (e.g. of the chip card or mobile phone), and
c) knowledge of the TAN or comparable password transmitted.

An accidental combination of these factors is nearly impossible, and even in this case successful access to the system would require intimate knowledge of the access procedure and the user ID, which is not given for access in the normal case. The user also has the option, in the event of loss of the chip card, to block his user ID immediately, or to have it blocked.

Another advantage of reliance on GSM is that the user can be reached at any point during the authorization process, for instance in case of access problems or doubt of his identity he can be called directly by the system administrator.

This solution has the advantage that it can be implemented very securely, cost-effectively, and with traditional, widely available, and secure hardware.

Another solution according to the invention is that the authorization computer and receiving unit are one device.

Additional advantages and application capabilitys of the invention result from the embodiment described below, in combination with the drawing.

An authorized user actuates a data input device (1). Using it, he sends the request for generation or selection and return of a TAN (or a comparable password) to an authorization computer (2). The authorization computer (2) generates the TAN (or comparable password). The telephone number or data

address, e.g. the email or network address of the receiver (3) of the user of the data input device (1) is known to the authorization computer (2). It sends this TAN (or comparable password) to a receiver (3) (not shown in more detail). The receiver (3) can be a pager (31) or a mobile phone (32). The receiver (3) can, however, also be the email address of a mailbox (not shown), a fax machine (33), or a speech output device. The speech output device can be a fixed speaker (34) or a telephone (35). The user reads this TAN (or comparable password) from the receiver (3) or hears it from the speech output, and enters it manually into the data input device (1). The data input device (1) now transmits the TAN (or comparable password) to the authorization computer (2). The authorization computer (2) checks whether this TAN (or comparable password) is still valid. For this purpose, the authorization computer can be programmed in such a way that the validity of the TAN (or the comparable password) is limited in time between its transmission to the receiver (3) and its transmission via the data input device (1). The time limitation could be two minutes, for instance. If the TAN (or comparable password) is valid, then the authorization computer (2) creates a connection to a receiving unit (4). Now the user is capable, for as long as this connection is maintained, to transmit data from the data input device (1) to the receiving unit (4) and/or to receive data.

It is obvious that this data can be encrypted for additional security.

It is also imaginable that not only the TAN (or comparable password) has a time limit on its validity, but that the length of time the connection will be maintained between the data input device (1) and the receiving unit (4) is also limited. This can prevent a "standing line" from being created between the data input device (1) and the receiving unit (4), which might itself constitute a security breach.

The authorization computer (2) and the receiving unit (4) can be a single computer. In that case, a first access is made to a data processing program which performs the authorization process (generation and transmission of the TAN) in the specified manner. Data transmission then occurs in a second step.

In fact, the data input device (1), the authorization computer (2), and the receiving unit (4) can be a single computer. In that case, there is a first access to a data processing program which performs the authorization process (generation and transmission of the TAN to the receiver) in the specified manner. Only after authorization does the user receive full computer access or access limited to certain areas.

List of reference numbers

1 Data input device
2 Authorization computer
3 Receiver
31 Pager
32 Mobile phone
33 Fax machine
34 Speaker
35 Telephone
4 Receiving unit

Patent claims

1. Process for authorization in data transmission systems using a transaction number (TAN) or a comparable password, characterized by the fact that
- in a first step, the user transmits through a data input device (1) his identification and/or an identification code for the data input device (1), together with a request for generation or selection of a TAN or comparable password from a file to an authorization computer (2),
- in a second step, the authorization computer (2) generates the TAN or comparable password or selects it from a file,
- in a third step, the authorization computer (3) transmits the TAN or comparable password over a different transmission path from that in step 1 to a receiver (1),
- in a fourth step, the user accepts this TAN or comparable password from the receiver (3) and enters it into the data input device (1),
- in a fifth step, this FAN or comparable password is transmitted back to the authorization computer (2),
- in a sixth step, the authorization computer (2) checks the validity of the TAN or comparable password, so that then
- in a seventh step, a connection can be made or released between the data input device (1) and a receiving unit (4).

2. Process according to Claim 1, characterized by the fact that the TAN or comparable password can only be used a single time.

3. Process according to one or more of Claims 1 through 2, characterized by the fact that the validity of the TAN or comparable password is a predefined user time.

4. Process according to one or more of Claims 1 through 3, characterized by the fact that the validity of the TAN or comparable password depends on a predefined under of files to be transmitted.

5. Process according to one or more of Claims 1 through 4, characterized by the fact that the validity of the TAN or comparable password depends on a predefined size of the files to be transmitted.

6. Process according to one or more of Claims 1 through 5, characterized by the fact that the access to the data input device (1) and/or the receiver (3) and/or the receiving unit (4) is protected by a password.

7. Process according to one or more of Claims 1 through 6, characterized by the fact that the data transmitted from the data input device (1) to the receiving unit (4), or in the other direction, is encrypted.

8. Process according to one or more of Claims 1 through 7, characterized by the fact that the data transmitted from the data input device (1) to the authorizing computer (2), or in the other direction, is encrypted.

9. System to execute the process according to one or more of Claims 1 through 8, characterized by the fact that the receiver (3) is a pager (31).

10. System to execute the process according to one or more of Claims 1 through 8, characterized by the fact that the receiver (3) is a mobile phone (32).

11. System to execute the process according to one or more of Claims 1 through 8, characterized by the fact that the receiver (3) is a fax machine (33).

12. System to execute the process according to one or more of Claims 1 through 8, characterized by the fact

that the receiver (3) is an email address or network address.

13. System to execute the process according to one or more of Claims 1 through 8, characterized by the fact that the receiver (3) is a speech output device.

14. System according to Claim 13, characterized by the fact that the speech output device is a speaker (34).

15. System according to Claim 13, characterized by the fact the the speech output device is a telephone (35).

16. System for execution of the process according to one or more of Claims 1 through 13, characterized by the fact that the receiver (3) is a radio receiver built into data input device (1), which displays the TAN or comparable password on the display or monitor of the data input device (1).

17. System according to Claim 14, characterized by the fact that the radio receiver has a user identification element.

18. System according to Claim 15, characterized by the fact that the user identification element is a magnetic or chip card.

19. System according to Claim 15, characterized by the fact that the user identification element works with graphical systems for inspection of a fingerprint or for image identification of the user.

20. System for the execution of the process according to one or more of Claims 1 through 17, characterized by the fact that matching encryption modules are present in the authorization computer (2) and the receiver (3).

21. System for the execution of the process according to one or more of Claims 1 through 18, characterized by the fact that the receiving unit (4) is a door locking mechanism.

22. System for the execution of the process according to one or more of Claims 1 through 19, characterized by the fact that the authorization computer (2) and the receiving unit (4) are integrated into a single device.

23. System for the execution of the process according to one or more of Claims 1 through 19, characterized by the fact that the data input device, the authorization computer (2), and the receiving unit (4) are integrated into a single device.

1 page(s) of drawings attached

Number: DE 197 18 103 A1
Int. Cl.[6]: H 04 L 9/32
Date of publication: June 4, 1996